UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,753	01/23/2001	Masao Kasahara	81942.0014	2712

26021 7590 06/01/2004	EXAMINER
HOGAN & HARTSON L.L.P. 500 S. GRAND AVENUE SUITE 1900 LOS ANGELES, CA 90071-2611	NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 January 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-14</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-14</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>23 January 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-14 are pending.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-2, 8-9, 11-14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Yanovsky US Patent No 5,703,948 in view of Orton US Patent No

5,297,206. Yanovsky discloses a protected communication method and system. Orton

discloses a cryptographic method for communication and electronic signatures.

4.   With regards to claims 1 and 13-14, Yanovsky discloses dividing a plaintext to be

encrypted into a plurality of divided plaintexts (Yanovsky, column 4 lines 20-23) and the

generation of ciphertext on a finite field (Yanovsky, column 4 lines 23-26), but fails to

teach the use of the product-sum type encryption and the use of public keys. Orton

discloses the use of the product-sum type encryption and the use of public keys (Orton,

column 12 lines 42-45, column 12 lines 56-58, and Figure 4). At the time the invention

was made, it would have been obvious to a person of ordinary skill in the art to utilize

Orton's encryption method with Yanovsky's cryptographic method because it offers the

advantage of ensuring secrecy of communication while minimizing the amount of

necessary computation and reducing the necessary key size (Yanovsky, column 4 lines 53-64, column 12 lines 48-51).

5.   With regards to claim 2, Yanovsky as modified teaches the divided plaintexts are encoded whereby each term of the intermediate decrypted text is constituted of an error correcting code word (Yanovsky, column 5 lines 7-14, Figure 1, and column 3 lines 12-18).

6.   With regards to claim 8, Yanovsky as modified teaches the decryption of divided plaintexts being performed sequentially starting from the lowest order term of the divided plaintexts of the ciphertext in ascending order (Orton, Figure 2).

7.   With regards to claim 9, Yanovsky as modified teaches the decryption of divided plaintexts being performed sequentially starting from the highest order term of the divided plaintexts of the ciphertext in ascending order (Orton, column 14 lines 53-61).

8.   With regards to claims 11 and 12, Yanovsky as modified teaches the inclusion of a communication channel for transmitting the generated ciphertext from one entity to another entity (Yanovsky, Figure 2) and a decryptor for decrypting the transmitted ciphertext into a plaintext (Yanovsky, Figure 1).

9.   Claims 3-7 and 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Yanovsky US Patent No 5,703,948 and Orton US Patent No 5,297,206 as applied to claim 1 above, and further in view of Boesch US Patent No 6,125,185. Boesch teaches a system for encryption key generation

10.   With regards to claim 3, Yanovsky as modified teaches the use of public keys for

each divided plaintext (Yanovsky, column 4 lines 20-26 and Orton, column 12 lines 42-

45, column 12 lines 56-58, and Figure 4), but fails to teach a plurality of keys previously

prepared and an arbitrary key being selected from among the prepared plurality of keys

for use in ciphertext generation. Boesch teaches a plurality of keys previously prepared

and an arbitrary key being selected from among the prepared plurality of keys for use in

ciphertext generation (Boesch, column 5 lines 1-21). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to utilize

Boesch's method of preparing a plurality of keys with Yanovsky's modified

cryptographic method because it offers the advantage of leveling processor loads by

shifting computationally complex operations out of the real-time cycle and allowing the

processor to generate those computationally complex factors during periods of less than

peak loading (Yanovsky, column 4 lines 63-67 and column 3 lines 43-47).

11.   With regards to claims 4-5 and 7, Yanovsky as modified teaches the public key

being fixed for a predetermined number (determined to be one) of divided plaintexts

(Yanovsky, column 4 lines 22-26).

12.   With regards to claim 6, Yanovsky as modified teaches the ciphertext being

generated such that the selection information for indicating the public key selected for

one divided plaintext is involved in another divided plaintext apart from the divided

plaintext by a predetermined number (Yanovsky, column 4 lines 34-43).

13.   With regards to claim 10, Yanovsky as modified teaches the decryption process

of dividing plaintext and the decryption process of selection information being carried

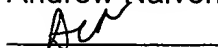out in parallel (Yanovsky, column 12 lines 48-51).

Conclusion

14.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L Nalven whose telephone number is 703 305

8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100